Money Matters

for People with Diverse Abilities

Workbook 6
Money safety

ABC LifeLiteracyCanada

Founding Sponsor

TD THE READY COMMITMENT

Money Matters

Welcome to *Money Matters!*

We designed *Money Matters* to help you take better care of yourself by taking better care of your money.

When you feel good about your money management, you're less stressed. You have more energy for the things that are important to you.

What will you learn?

In today's workshop, you will learn about:

- **Online safety**
- **Phishing scams**
- **Identity theft**
- **Financial abuse**

ABC LifeLiteracyCanada

What is money safety?

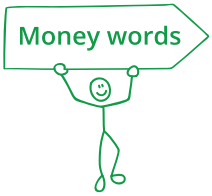
Money safety is everything you can do to protect your money and your personal information.

Activity

Thinking about money safety

Here are some people talking about how they use their money and personal information. Do you think they're being safe or unsafe? Circle your answer.

"I only carry as much **cash** as I need. "	**Safe**	**Unsafe**	**Not Sure**
"I use a **PIN** that's easy to guess, in case I forget it."	**Safe**	**Unsafe**	**Not Sure**
"I use the public computer at the library for **online banking**."	**Safe**	**Unsafe**	**Not Sure**



Cash is paper money and coins.

PIN is short for "Personal Identification Number." Your PIN is your password to use your debit card.

Online banking is when you use a computer to do your banking over the internet.

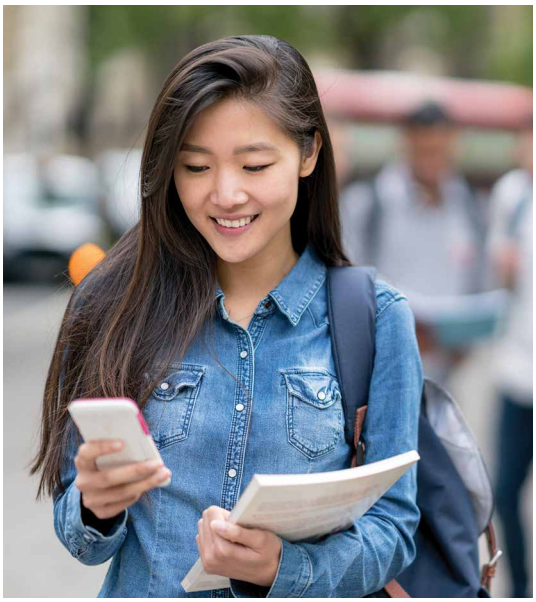
A **debit card** is a card from the bank that lets you spend money from your bank account.

"I use my neighbour's smartphone for **mobile banking**."	**Safe**	**Unsafe**	**Not Sure**
"When I'm worried about how safe my money is, I talk to someone I trust."	**Safe**	**Unsafe**	**Not Sure**

Mobile banking is when you use a tablet or smartphone to do your banking.

Let's talk about it

Did anyone in your group circle different answers than you? Why did they choose their answer?



Keeping your money and personal information safe

Here are some tips that might help you keep your money and personal information safe.

Carry only as much cash as you need
If you carry a lot of **cash**, it might get lost or stolen.

Use passwords and PINs that are hard to guess
If your password or **PIN** is too simple, dishonest people might guess it. If someone else can guess your password or **PIN**, they can steal your money and your personal information.

Use a private computer (like a computer at home, if you have one) for online banking
Dishonest people can steal information from public computers.

The next page has more tips to help you keep your money and personal information safe!

Here are some more tips that might help you keep your money and personal information safe.

Use a private internet connection (like your internet at home, if you have it) for online and mobile banking
Dishonest people can steal information from public internet connections.

Only use your personal smartphone or the smartphone of someone you trust for mobile banking
Smartphones sometimes save your information. If a dishonest person uses the same smartphone, they can steal your information.

Talk to someone you trust if you're not sure
Sometimes it's hard to tell if something is safe or unsafe. Try talking to someone you trust or a bank worker about money safety.

Why is money safety important?

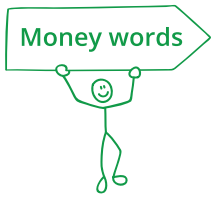
Money safety means protecting your money and your **identity**. If your money and your **identity** aren't safe, dishonest people could steal them from you.

In the rest of this book, we're going to learn more about protecting your money and your **identity**.

Protecting your identity

It's very important to protect your **identity**. Your personal information is private, and you should only share it with people you trust.

If dishonest people steal your personal information, they can pretend to be you. This is a crime called **identity theft**.



Your **identity** is all your personal information. Your identity can include:

- Your full name
- Your birthdate
- Your Social Insurance Number (SIN)
- All your passwords

Identity theft is a kind of crime where dishonest people steal someone's personal information and then pretend to be that person.

Who do you trust?

Who are the people you trust with your personal information? Here is a list of some people you might trust.

Remember, everyone trusts different people. You don't have to trust everyone on this list.

- Your parents
- Your brothers and sisters
- Your kids
- Bank workers
- Government workers
- Your best friend

Is there anyone else you trust with your personal information?

Did you know?

You have the right to keep your money and your personal information safe. No one is allowed to take your money or your personal information without your permission.

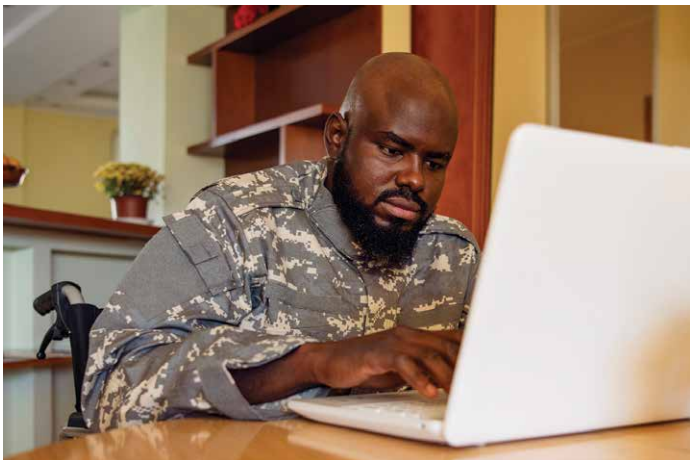
Online banking and mobile banking

Online banking means using a computer to do your banking over the internet. **Mobile banking** means using a smartphone or a tablet to do your banking.

Here are some things you can do with **online** and **mobile banking**:

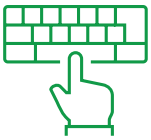
- Check your bank account activity and balance
- Pay your bills online
- Move money between your bank accounts
- Send money to other people through **e-transfers**

An **e-transfer** means sending money to someone else over the internet using a computer, a tablet, or a smartphone.



Different banks let you do different things with **online banking**, like open a new account or pay your bills. You can visit or call your bank to ask them about their **online** and **mobile banking** services.

Activity



Making a strong password

It's important to create a strong password when you sign up for **online** and **mobile banking**. A weak password is easy for someone else to guess, but a strong one isn't easy to guess. A strong password has a mix of:

- numbers **2 67 91**
- small letters **c g k**
- capital letters **F Z H**
- symbols **! $ # ?**

Here are some examples of passwords. Do you think these passwords are strong or weak?

abc123	**Strong**	**Weak**	**Not Sure**
odCD7c#21	**Strong**	**Weak**	**Not Sure**
password	**Strong**	**Weak**	**Not Sure**
1111111	**Strong**	**Weak**	**Not Sure**
83!feS3%	**Strong**	**Weak**	**Not Sure**
E35!?fri3O	**Strong**	**Weak**	**Not Sure**

Online and mobile banking safety

Here are some more ways to keep your bank account safe online:

- Only use your bank's official website or app for **online** or **mobile banking**
- Don't tell anyone your **online** or **mobile banking** username or password
- Avoid using public computers or public internet connections to do your **online** or **mobile banking**
- Ask a bank worker if there are other ways to keep your bank account safe

Meet Ali

Ali works hard to protect his **identity**:

- He uses strong passwords that are hard to guess
- He rips up papers with personal information before he recycles them
- He only shares personal information with his parents, bank workers, and government workers

Let's talk about it

Do you use the same tricks as Ali to protect your **identity**?
What else can you do to protect your **identity**?

Notes:

Ali's story

Ali just started to use **online banking**. He's happy, because now it's easy to see how much money he has. He also likes paying his bills online.

One day, Ali gets an email. It says:

LB

From: Local Bank <local-bank@gr564.com>
Subject: Action required – Information incomplete
Date: Thu 2020-02-13 12:56AM
To: Ali

< >>

Dear Customer,

This email is to inform you that your online banking porfile with Local Bank is incomplete. Click on the link below and enter your banking password to complete your porfile.

http://info.localbank.ca/completeprofile

Sincerely,

LOCAL BANK

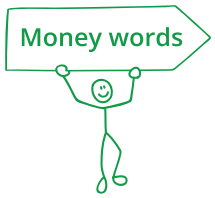
"This email looks serious," says Ali. "I wonder if I should give them my password?"

Let's talk about it

Do you think it's safe for Ali to share his banking password? Why or why not?

Phishing

Ali's email is a kind of **scam** called **phishing**.



A **scam** is an illegal plan to trick people and steal from them.

Phishing is a scam that uses email, phone calls, or text messages. Phishing scams try to steal personal information from you. They usually pretend to be from someone or someplace you trust, like a family member or your bank.

Here are some clues that an email is **phishing**. Can you find these clues in Ali's email?

1.

Date: Thu 2020-02-13 12:56AM
To: Ali

Dear Customer,

This email is to inform you that your

Sometimes **phishing** emails don't use your name. **Phishing** emails might use a different word, like "Customer."

2.

orm you that your online banking porfile
incomplete. Click on the link below and
password to complete your porfile.

Phishing emails often have mistakes in them, like words that are spelled wrong. A professional email probably won't have mistakes in it.

3.

with Local Bank is incomplete. Click on the link below
enter your banking password to complete your porfile

Phishing emails usually ask you for personal information. Banks don't ask for your personal information in emails or text messages. You should never give out personal information online or in text messages.

4. enter your banking password to complete your porfile
http://info.localbank.ca/completeprofile

Phishing emails might send you to a website where they will steal your personal information. Sometimes, the website says **http://**. Usually, official websites say **https://** instead of **http://**. The extra "s" stands for "secure."

5. Sincerely,
LOCAL BANK

Phishing emails try to look like they're really coming from your bank, or another trusted source. Even if an email has the right logo or their email address looks right, you might have a **phishing** email.

Here are some more clues that an email might be a **phishing scam**:

- The email warns you about suspicious activity on your account
- The email says there's a problem with your account
- The email says you're eligible for a tax refund or free stuff
- The email says the problem is urgent and you have to respond quickly

Ali thinks he got a **phishing** email. He phones his bank, and the bank worker says Local Bank didn't send that email.

Ali deletes the **phishing** email.

Ali's personal information is safe!

Phishing scams: What to do

Here's what you should do if you think an email is a **phishing scam**:

- **If you get an email and you think it's a scam, don't share any information with them!**
- **Search online for the organization's phone number. Contact the organization and ask if they sent you an email**
- **Don't open any attachments or click on any links in the email**
- **Don't reply to the email**
- **Mark the email as spam**
- **Delete the email**

Sometimes **phishing scams** come from text messages or phone calls. A text message or phone call might be **phishing** if:

- it's from someone you don't know
- you weren't expecting the call or text message

If you think a call or a text message is **phishing**, don't share any information with them!

Let's practice

Here is another **phishing** email. Can you spot any clues that this email is a **scam**?

On your own or with a friend, try to circle some clues that this email is a **phishing scam**.

CR

From: Canada Revenue Agency <tax-refund@can.gov.agancy.com>
Subject: Tax Refund
Date: Fri 2020-02-28 03:15PM
To: Tax Payer

< >>

Canada Revenue Agency

Canada

Canada Revenue Agency

Dear Tax Payer,

After a review of your 2018 tax forms, we have determined that you are eligable for a tax refund of $362.58.

To claim your refund, fill out the form on the canada revenue agency website: http://canada-rev-agency.com.

Sincerely,

Canada Revenue Agency

Let's talk about it

Did anyone in your group find different clues?

Why did they pick those clues?

Identity theft: What to do

Even when we work hard to protect our information, sometimes people find a way to steal it. Here's what to do if you think someone has stolen your personal information.

What did they steal?	What should you do?
Your bank information, **credit card**, or **debit card**	**Contact your bank.** You can visit in person, or call the phone number on your last bank or **credit card** statement. A bank worker will tell you what to do next.
Your other personal information	**Contact the police and your bank.** Tell the police and your bank that you'd like to report **identity theft**. You can visit in person, or phone them. They will tell you what to do next.

A **credit card** is a card that lets you buy now and pay later.

Other ways to protect your identity

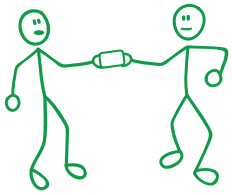
- Rip up papers with your personal information before you throw them out
- Use passwords that are hard to guess, and don't write them down
- Don't share your Social Insurance Number with anyone you don't trust
- If people ask you to spend money or share information that makes you uncomfortable, say no
- You are always allowed to talk to someone you trust before you make big decisions

Financial abuse

Financial abuse happens when someone you trust uses your money, your belongings, or your **identity** without your permission.

This is financial abuse

Ali's friend Kathy used Ali's **credit card** to buy some clothes. Kathy isn't allowed to use Ali's **credit card**, but she used it anyway. Ali doesn't know if Kathy will pay him back.



This is **not** financial abuse

Ali's brother, Mohammed, asks for permission to borrow Ali's **credit card**. Ali says yes, and Mohammed pays him back right away.

Signs of financial abuse

Sometimes it can be hard to tell if financial abuse is happening. These questions can help you understand if you're going through financial abuse.

Circle the answer in the box that sounds true to you.

Does someone else use your money without your permission?	**Yes**	**No**	**Not Sure**
If someone else makes decisions about your money, do they hide information or lie about your money?	**Yes**	**No**	**Not Sure**
Do your money or other belongings go missing?	**Yes**	**No**	**Not Sure**
Do you feel like someone is trying to cut you off from everyone else you know?	**Yes**	**No**	**Not Sure**
Does someone else keep your money away from you, even though they're not supposed to?	**Yes**	**No**	**Not Sure**

Did you answer "Yes" or "Not sure" to any questions?

You might be going through financial abuse. The next page tells you what to do.

Did you answer "No" to every question?

That's great! Remember to keep your money and your personal information safe.

Financial abuse: What to do

Do you think you're going through financial abuse? Do you think someone you know is going through financial abuse?

Here's what to do.

It's important to tell someone that you think you're going through financial abuse. Talk to someone you trust, such as:

- a family member
- a close friend
- a bank worker at your bank
- your doctor

If you feel like you're in immediate danger, call the police and ask for help.

Do you want to make sure you're safe from financial abuse? Here are some things you can do:

- **Keep track of your money**
  Write down all the money you spend or give away to help you keep track of your money.
- **Ask for help with important decisions**
  Ask someone you trust to look at contracts or other important agreements before you sign them.
- **Keep in touch with family and friends**
  It's important to have lots of people you can talk to and who can help you.

Money safety

What we learned today

Today we learned about:

- Online safety
- Phishing scams
- Identity theft
- Financial abuse

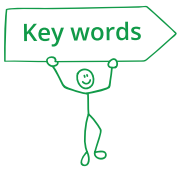
Remember

You have the right to keep your money and your personal information safe. No one is allowed to take your money or your personal information without your permission.

Practice on your own

Think about something you can do today to make your money and personal information safer. Maybe you can track your spending, or make your **online banking** password stronger. If you know what you want to do, write it down here.

I'm going to make my money and personal information safer by:



Cash	Paper money and coins
Credit card	A card that lets you buy now and pay later
Debit card	A card from the bank that lets you spend money from your bank account
E-transfer	Sending money to someone over the internet using a computer, a tablet, or a smartphone
Identity	All your personal information. Your identity can include: • Your full name • Your birthdate • Your Social Insurance Number (SIN) • All your passwords
Identity theft	A kind of crime where dishonest people steal someone's personal information and then pretend to be that person
Mobile banking	Using a tablet or smartphone to do your banking

Online banking	Using a computer to do your banking over the internet
Phishing	Phishing is a scam that uses email, phone calls, or text messages. Phishing scams try to steal personal information from you. They usually pretend to be from someone or someplace you trust, like a family member or your bank
PIN	Short for "Personal Identification Number." Your PIN is your password to use your debit card
Scam	An illegal plan to trick people and steal from them

Learning more

The Government of Canada has a "Little Black Book of **Scams**" that tells you how to spot **scams** and how to deal with them.
https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

TD Bank has more information about online **scams**, including tips for protecting your computer and how to prevent **scams**.
https://www.td.com/privacy-and-security/privacy-and-security/how-you-can-protect-yourself/protect-yourself.jsp

ABC Life Literacy Canada has online resources to help you learn more about money management.
https://abcmoneymatters.ca/about/#mmpwda

Thank you for participating in *Money Matters for People with Diverse Abilities*!

ABC LifeLiteracyCanada

Founding Sponsor
TD THE READY COMMITMENT